

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN**

SUSAN GIASSON,

Plaintiff,

v.

MRA – THE MANAGEMENT
ASSOCIATION, INC.,

Defendant.

Case No. 24-CV-839-JPS

ORDER

1. INTRODUCTION

In July 2024, Plaintiff Susan Giasson (“Plaintiff”), individually and on behalf of a putative class, sued Defendant MRA – The Management Association, Inc. (“Defendant”) for negligence; negligence per se; breach of implied contract; invasion of privacy; unjust enrichment; breach of fiduciary duty; violation of the Wisconsin Deceptive Trade Practices Act (“WDTPA”), Wis. Stat. §§ 100.18 et seq.; and violation of Wis. Stat. § 146.82, which protects the confidentiality of patient health records. ECF No. 1 at 25–42. She seeks declaratory relief, injunctive relief, and damages. *Id.* at 42–44.

Defendant now moves to dismiss the complaint on the grounds that (1) it fails to properly allege that Plaintiff has standing to seek declaratory or injunctive relief; and (2) it fails to state any claim upon which relief can be granted. ECF No. 14. The motion is fully briefed. ECF Nos. 15, 18,¹ 20.

¹Plaintiff included roughly four pages worth of facts in its opposition to the motion to dismiss in contravention of the Court’s directive that the parties “omit a facts section from their briefing.” ECF No. 18 at 3–7; ECF No. 2 at 4. Defendant

For the reasons discussed herein, the Court will grant the motion in part and deny it in part.

2. LEGAL STANDARDS

The Court notes at the outset that in considering a motion to dismiss filed before a putative class has been certified, the Court looks only to the named Plaintiff's individual claims and circumstances. *Crissen v. Gupta*, 994 F. Supp. 2d 937, 945 (S.D. Ind. 2014) (citing *Tatum v. Chrysler Grp. LLC*, No. 10-4269 (ES), 2012 U.S. Dist. LEXIS 171746, at *11–12 (D.N.J. Dec. 3, 2012); *Tillman v. U.S. Energy Sav. Corp.*, No. 08 C 1641, 2008 U.S. Dist. LEXIS 53313, at *10 (N.D. Ill. July 14, 2008); and *Chambers v. Am. Trans Air*, 17 F.3d 998, 1006 (7th Cir. 1994)).

2.1 Lack of Standing

“Questions of standing are appropriately addressed via a motion to dismiss under [Federal] Rule [of Civil Procedure] 12(b)(1) for lack of subject-matter jurisdiction.” *Swanigan v. City of Chicago*, 881 F.3d 577, 582 (7th Cir. 2018) (citing *Berger v. NCAA*, 843 F.3d 285, 289 (7th Cir. 2016)). “If the plaintiff lacks standing, the federal court lacks subject matter jurisdiction and the suit must be dismissed” *Int’l Union of Operating Engr’rs, Local 139 v. Daley*, 983 F.3d 287, 294 (7th Cir. 2020) (quoting *Taylor v. McCament*, 875 F.3d 849, 853 (7th Cir. 2017)).

2.2 Failure to State a Claim

Federal Rule of Civil Procedure 12(b)(6) also provides for dismissal of complaints that fail to state a viable claim for relief. To state a claim, a

also represents in its motion that Plaintiff failed to participate in the joint jury instruction submission requirement. ECF No. 14 at 1 n.1; *see also* ECF No. 2 at 5. The Court’s protocols are designed to facilitate streamlined and efficient litigation, and the Court expects parties to adhere to them. Future failures to comply with the Court’s protocols may result in sanctions as appropriate.

complaint must provide “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). In other words, the complaint must give “fair notice of what the . . . claim is and the grounds upon which it rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). The allegations must “plausibly suggest that the plaintiff has a right to relief, raising that possibility above a speculative level.” *Kubiak v. City of Chicago*, 810 F.3d 476, 480 (7th Cir. 2016) (quoting *EEOC v. Concentra Health Servs., Inc.*, 496 F.3d 773, 776 (7th Cir. 2007)). Plausibility requires “more than a sheer possibility that a defendant has acted unlawfully.” *Olson v. Champaign County*, 784 F.3d 1093, 1099 (7th Cir. 2015) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). A plausible claim is one with “enough fact to raise a reasonable expectation that discovery will reveal evidence” supporting the plaintiff’s allegations. *Twombly*, 550 U.S. at 556.

In reviewing the complaint, the Court is required to “accept as true all of the well-pleaded facts in the complaint and draw all reasonable inferences in favor of the plaintiff.” *Kubiak*, 810 F.3d at 480–81 (citing *Tamayo v. Blagojevich*, 526 F.3d 1074, 1081 (7th Cir. 2008)). At the motion to dismiss stage, the Court does not ask “did these things happen”; instead, “the proper question to ask is . . . ‘could these things have happened.’” *Olson*, 784 F.3d at 1099 (quoting *Carlson v. CSX Transp., Inc.*, 758 F.3d 819, 827 (7th Cir. 2014)). In any event, the Court “need not accept as true ‘legal conclusion[s], or t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements.’” *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009) (quoting *Iqbal*, 556 U.S. at 678). Ultimately, dismissal is only appropriate “if it appears beyond doubt that the plaintiff could prove no set of facts in support of his claim that would entitle him to the relief

requested.” *Enger v. Chi. Carriage Cab Corp.*, 812 F.3d 565, 568 (7th Cir. 2016) (quoting *R.J.R Servs., Inc. v. Aetna Cas. & Sur. Co.*, 895 F.2d 279, 281 (7th Cir. 1989)).

3. FACTS²

Defendant is a nonprofit employer association that serves more than 5,000 employers, covering more than 1 million employees worldwide. As such, Defendant stores highly sensitive personal identifiable information (“PII”) and protected health information (“PHI”) about its clients’ current and former employees.

Upon information and belief, Plaintiff’s current and/or former employer is or was a client of Defendant. As a condition of her employment, Plaintiff (or her third-party agent) provided Defendant with her PII/PHI, and Defendant used that PII/PHI to facilitate its business. Defendant thus obtained and maintained Plaintiff’s PII/PHI. Plaintiff trusted that Defendant would use reasonable measures to protect her PII/PHI, and she understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for cybersecurity and protection of her PII/PHI.

Under state and federal law, businesses like Defendant have duties to protect clients’ current and former employees’ PII/PHI and to notify them about breaches. Defendant recognizes these duties in its “Privacy Policy.”

²This summary of facts is drawn from the operative complaint, ECF No. 1, as required at this stage. *Carroll v. Morrison Hotel Corp.*, 149 F.2d 404, 407 (7th Cir. 1945) (“Ordinarily upon a defendant’s motion to dismiss, the court may consider only the allegations in the complaint.”). Citations thereto are omitted. Facts not relevant to the pending motion are also omitted. The Court also notes as a general matter that many of Plaintiff’s factual allegations are vague and their meaning is not entirely clear to the Court.

Similarly, Defendant promises in its “MRA Background Checking Policy” that it will, among other things, “take reasonable steps to verify an individual’s identity before granting access to [PII].” In collecting and maintaining PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law, and it positions itself as an expert on cybersecurity in its advertisements. Plaintiff and the putative class members themselves took reasonable steps to secure their PII/PHI.

On or around July 29, 2023, Defendant was hacked in a data breach, allegedly causing “widespread injury and monetary damages.” Plaintiff alleges that Defendant knew, or should have known, of the risk of the data breach given the increased prevalence and notoriety of such breaches in recent years.

Defendant admitted that its investigation determined that “an unknown party acquired certain information on parts of [its] network.” It is unknown for precisely how long the cybercriminals had access to Defendant’s network. In a disclosure to Massachusetts authorities, Defendant stated that “[o]n July 29, 2023, [Defendant] experienced a network disruption event.” But in a disclosure to the Maine Attorney General, Defendant stated that the data breach lasted from June 30, 2023 to July 29, 2023. It therefore appears that the breach began on June 30, 2023, but that Defendant was unable to detect it until July 29, 2023.

Because of the data breach, many types of PII/PHI were compromised, including dates of birth, financial account information, medical information, and Social Security numbers. At least 3,477 persons’ PII/PHI was exposed in the data breach. Plaintiff is a victim of the data breach, having received a Notice of Data Breach on or around July 3, 2024.

ECF No. 1-1.³ Defendant did not, or could not, specify in the Notice of Data Breach “the full scope” of the breach, as it had been “unable to determine precisely what information was stolen and when.” Nevertheless, the Notice of Data Breach that Plaintiff received stated that “[t]he information potentially impacted . . . included” Plaintiff’s name and her Social Security number.

Defendant waited until May 9, 2024—285 days after the breach was discovered—to notify affected persons of the breach. This deprived Plaintiff and the other putative class members of the opportunity to try to mitigate their injuries in a timely manner. When Defendant did finally notify Plaintiff and the other putative class members, it acknowledged that the breach posed a continuing and significant risk of identity theft. It accordingly offered twelve months’ worth of credit monitoring and identity protection services.

Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its clients’ current and former employees’ PII/PHI. Cybercriminals were able to breach Defendant’s system because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols. Defendant failed to follow industry standards and Federal Trade Commission (“FTC”) guidelines on data security, and this contributed to the breach. Plaintiff also

³The Court may properly consider this Notice of Data Breach at the motion to dismiss stage. *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013) (noting that, on a motion to dismiss, a court may consider documents that are attached to the complaint (collecting cases)).

alleges that Defendant's security failures violated the Health Insurance Portability and Accountability Act ("HIPAA").

The cybercriminals that obtained Plaintiff's and the putative class members' PII/PHI appear to be a part of the cybercriminal group "Abyss," which "host[s] a TOR-based website where victims are listed along with their exfiltrated data should they fail to comply with the demands of the threat actor." Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. Abyss has already published 3 TB worth of PII/PHI from the data breach on the dark web. Abyss published various links to the data—along with the access password—on the dark web. Accordingly, on information and belief, Plaintiff's and the other putative class members' PII/PHI has already been published, or will imminently be published, by Abyss on the dark web.

Since the breach, Defendant has "implemented additional technical safeguards and is working with outside specialists to continually monitor all [its] system[s]." Defendant has not, however, explained what "additional technical safeguards" entails, leaving Plaintiff and other putative class members to fear that their PII/PHI remains unsecure. Plaintiff accordingly requests that Defendant be required to implement adequate cybersecurity consistent with industry standards.

Plaintiff alleges that the breach has "inflict[ed] numerous injuries and significant damages upon Plaintiff and [the putative] [c]lass members." Plaintiff has spent, and will continue to spend, significant time and effort monitoring her accounts to protect herself from identity theft. Following the breach, she has suffered from a spike in spam and scam emails. As a result of the breach, she fears for her personal financial security and suffers anxiety, sleep disruption, fear, and frustration, and suffered injury in the

form of damages to and diminution in value of her PII/PHI. She also suffers “imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft” because of the breach. She and the other putative class members have also suffered, or are at increased risk of suffering, from delay in receipt of tax refund monies and lost wages from spending time trying to mitigate the fallout of the breach, among other harms.

4. LAW AND ANALYSIS

4.1 Lack of Standing to Seek Declaratory or Injunctive Relief

Defendant first argues that Plaintiff lacks standing to seek declaratory or injunctive relief. ECF No. 15 at 8.

“The plaintiffs, as the parties invoking federal jurisdiction, bear the burden of establishing the required elements of standing.” *Remijas v. Neimas Marcus Grp., LLC*, 794 F.3d 688, 691 (7th Cir. 2015) (quoting *Reid L. v. Ill. State Bd. of Educ.*, 358 F.3d 511, 515 (7th Cir. 2004)). “A plaintiff must demonstrate standing for each form of relief sought.” *Kenseth v. Dean Health Plan, Inc.*, 722 F.3d 869, 890 (7th Cir. 2013)); *see also Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996) (“[S]tanding is not dispensed in gross.”). “In order to have standing, a litigant must ‘prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct and is likely to be redressed by a favorable judicial decision.’” *Remijas*, 794 F.3d at 691–92 (quoting *Hollingsworth v. Perry*, 570 U.S. 693, 704 (2013)). “If ‘the plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve.’” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021) (quoting *Casillas v. Madison Ave. Assocs., Inc.*, 926 F.3d 329, 333 (7th Cir. 2019)).

Defendant specifically argues that Plaintiff cannot demonstrate redressability. ECF No. 15 at 8–9 (citing *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 378 (1st Cir. 2023) and *Stencil v. Johnson*, 605 F. Supp. 3d 1109 (E.D. Wis. 2022)). With respect to her request for injunctive relief, Defendant contends that Plaintiff’s “allegations of future injury are too hypothetical to support standing for injunctive relief” and that “her request for injunctive relief . . . is not likely to redress her alleged injuries.” *Id.* at 8 (citing *Webb*, 72 F.4th at 378); *see also* ECF No. 20 at 6–8. Similarly, with respect to her request for declaratory relief, Defendant argues that “[a] declaration that ‘Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it’ would not[] provide any relief to Plaintiff.” ECF No. 15 at 9 (citing ECF No. 1 at 42–43).

In opposition, Plaintiff maintains that “injunctive relief is critical to prevent future breaches” and that “Plaintiff sufficiently alleges ongoing security deficiencies that continue to expose sensitive data to future breaches.” ECF No. 18 at 8 (citing ECF No. 1 at 9, 15, 28, and 35); *id.* (also arguing that “injunctive relief can mitigate the risks stemming from the breach”). Plaintiff does not respond specifically regarding Defendant’s contention that the sought declaration “would not[] provide any relief to Plaintiff.” ECF No. 15 at 9 (citing ECF No. 1 at 42).

4.1.1 Standing to Seek the Injunctive Relief Described in the Complaint

The Court begins with the argument that Plaintiff lacks standing to seek the Court to enjoin Defendant “to use adequate security consistent with industry standards to protect the data entrusted to it.” ECF No. 1 at 43. “Because an injunction is a forward-looking remedy, a plaintiff seeking this form of relief has standing to sue for an alleged future

injury only if ‘the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.’” *Swanigan*, 881 F.3d at 583 (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted)). For purposes of seeking injunctive relief, “[p]ast injury alone is insufficient,’ as is a threat of injury that is ‘merely conjectural or hypothetical.’” *Id.* (quoting *Simic v. City of Chicago*, 851 F.3d 734, 738 (7th Cir. 2017)).

Plaintiff argues that the sought injunctive relief is critical to preventing future breaches, but her complaint does not plausibly allege that another breach of Defendant’s network is “certainly impending.” *Swanigan*, 881 F.3d at 583 (citation omitted). She emphasizes the increased prevalence of data breaches in recent years, particularly in the healthcare field, ECF No. 1 at 17–18, but none of the data or information in her complaint addresses the likelihood of the same entity network being breached a second time. *See Dusterhoft v. Onetouchpoint Corp.*, No. 22-cv-0882-bhl, 2024 U.S. Dist. LEXIS 170993, at *26–27 (E.D. Wis. Sept. 23, 2024) (“Plaintiffs provide only scant conclusory allegations concerning the risk that they will suffer from another data breach at OneTouchPoint. . . . Plaintiffs allege no specific facts establishing how OneTouchPoint’s data security remains inadequate, or how they face a real and immediate threat of future injury from another data breach occurring due to OneTouchPoint’s failure to protect their data.”); *see also Hall v. Centerspace, LP*, No. 22-cv-2028 (KMM/DJF), 2023 U.S. Dist. LEXIS 83438, *10–11 (D. Minn. May 12, 2023) (“[T]he injunction would be aimed at decreasing the likelihood of a future data breach that could expose the sensitive data . . . [but] there are no facts in the Complaint that indicate a second data breach is certainly impending, or even that there is a substantial risk one will occur. . . . Nothing in [the] pleading transforms the

possibility that [the defendant] might suffer another data breach into an imminent or substantial risk.”). Indeed, Plaintiff’s allegation that “[s]ince the breach, Defendant ‘has since implemented additional technical safeguards and is working with outside specialists to continually monitor all [its] system[s],’” ECF No. 1 at 9, undercuts the likelihood that Defendant’s system will be again breached. *Webb*, 72 F.4th at 378 (“[A]ny available inference that [the defendant’s] prior data breach might make a future data breach more likely is undercut by the plaintiff’s own allegation that ‘[f]ollowing the [d]ata [b]reach, [defendant] implemented new security safeguards to prevent and mitigate data breaches’”).

The Court also agrees with Defendant that enjoining it to “use adequate security consistent with industry standards to protect the data entrusted to it” will not redress Plaintiff’s alleged injuries. ECF No. 15 at 8; ECF No. 1 at 43. To demonstrate redressability, the plaintiff must show “a ‘substantial likelihood’ that the requested relief will remedy the alleged injury in fact.” *Vt. Agency of Nat’l Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 771 (2000) (quoting *Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 41 (1976)). “Redressability turns on the ‘connection between the alleged injury and the judicial relief requested.’” *Pavlock v. Holcomb*, 35 F.4th 581, 588 (7th Cir. 2022) (quoting *Allen v. Wright*, 468 U.S. 737, 753 n.19 (1984)).

The problem here is that the breach has already occurred, and the data is already on the dark web, where—irrespective of if Defendant is enjoined to strengthen its security systems to protect the data to which it is entrusted—it is susceptible to access for nefarious purposes. Enjoining Defendant to improve its data security measures cannot change that fact because, as Plaintiff notes, the exposure of her data is “a bell that cannot be unrung.” ECF No. 1 at 2. Plaintiff alleges that she continues to have to spend

significant time and effort monitoring her accounts, that she now experiences a spike in spam and scam emails and calls, and that she now faces an increased risk of identity theft and fraud, but enjoining Defendant to improve its data security measures will not redress those injuries because Plaintiff's data was already exposed. *See Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *27 ("[W]hile Plaintiffs may face a continuing threat of harm from the breach that has already occurred, an injunction requiring [the defendant] to change their data security practices will not redress those injuries."); *Webb*, 72 F.4th at 378 ("[A]n injunction requiring [the defendant] to improve its cybersecurity systems cannot protect the plaintiffs from future misuse of their PII by the individuals they allege now possess it. Any such relief would safeguard only against a future breach."). Plaintiff's complaint itself acknowledges the fact that her requested injunctive relief is applicable only in the context of another data breach, which, again, she has not demonstrated is "certainly impending." ECF No. 1 at 43 ("If an injunction is not issued, Plaintiff . . . will suffer irreparable injury and lack an adequate legal remedy *if Defendant experiences a second data breach.*" (emphasis added)); *Swanigan*, 881 F.3d at 583.

The cases upon which Plaintiff relies in support of her contention that she has standing to pursue injunctive relief are distinguishable. ECF No. 18 at 8 (collecting cases). The court in *Remijas*, for example, did not analyze the standing issue specifically in the context of a request for injunctive relief. *See generally* 794 F.3d 688. That matters because, as earlier noted, "a plaintiff must demonstrate standing for each form of relief sought." *Kenseth*, 722 F.3d at 890. Accordingly, to the extent that the Court questions whether the sought injunctive relief would redress Plaintiff's alleged injuries, *Remijas* provides little to no guidance. *In re Fortra File*

Transfer Software Data Security Breach Litigation is also distinguishable. See ECF No. 18 at 8. There, the plaintiffs' sought injunctive relief included a request that the defendants "provide lifetime credit monitoring and identity theft insurance." Nos. 24-MD-03090-RAR and 23-cv-60830-RAR, 2024 U.S. Dist. LEXIS 169281, at *39 (S.D. Fla. Sept. 18, 2024). That sort of injunctive relief does not present the same redressability issue as that requested in Plaintiff's complaint because, unlike Plaintiff's request that Defendant be required to improve upon its security system to protect the data entrusted to it, lifetime credit monitoring and identity theft insurance would redress the harms associated with the fallout of the breach that has already occurred (potential identity theft, fraud, etc.). Plaintiff does not seek the sort of injunctive relief sought in *Fortra*; indeed, Defendant has already offered credit monitoring and identity protection services to her. ECF No. 1-1 at 2; see ECF No. 20 at 7 (Defendant's reply) ("Plaintiff's argument that the Court could award 'credit monitoring and dark web surveillance' . . . is disingenuous because the exhibit she attached to the Complaint specifies [that Defendant] already offered her 'credit monitoring and identity protection services at no cost . . . '" (quoting ECF No. 1-1 at 2)).

For all these reasons, the Court concludes that Plaintiff lacks standing to pursue the injunctive relief described in her complaint. ECF No. 1 at 43; see *Ramsay v. Mayer*, 420 F. App'x 586, 588 (7th Cir. 2011) ("If plaintiffs indeed lack standing, . . . then dismissal must be *without* prejudice" (citing *Steel Co. v. Citizens for Better Env't*, 523 U.S. 83 (1998))).

4.1.2 Standing to Seek the Declaratory Relief Described in the Complaint

The Court next addresses the argument that Plaintiff lacks standing to pursue declaratory relief. ECF No. 15 at 9. "The purpose of declaratory

judgment is to deprive the defendant of delay as a weapon by declaring the parties' legal rights in anticipation of some future conduct." *Thompson v. Ortiz*, 619 F. App'x 542, 544 (7th Cir. 2015) (citing *Med. Assurance Co. v. Hellman*, 610 F.3d 371, 377 (7th Cir. 2010)). "A plaintiff lacks standing to seek declaratory judgment where a declaration of the parties' legal rights will provide no relief." *Id.* (citing *Bontkowski v. Smith*, 305 F.3d 757, 761 (7th Cir. 2002) and *Perry v. Sheahan*, 222 F.3d 309, 313–14 (7th Cir. 2000)).

It is unclear how Plaintiff's sought declaration—essentially, that Defendant breached its duty to use reasonable measures to protect the PII/PHI entrusted to it—would redress the injuries alleged in the complaint. *See Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *28 ("Plaintiffs have alleged injuries sufficient to support standing stemming . . . from a data breach that has already occurred. . . . Plaintiffs' requested declaratory relief would do nothing to redress those injuries. Declarations that [the defendant] breached a duty it owed them or otherwise acted unlawfully would not, standing alone, provide any relief to Plaintiffs."); *see also Jenkins v. Associated Wholesale Grocers, Inc.*, No. 24-4039-DDC-GEB, 2025 U.S. Dist. LEXIS 39481, at *36–39 (D. Kan. Mar. 5, 2025) (concluding that the plaintiff lacked standing to seek a declaration that the "defendant owes a duty to secure the proposed class's PII [and that the] defendant continues to breach that duty by failing to employ reasonable measures to secure the proposed class's PII" because that declaratory relief focused on "the risk that [the] defendant will face *another* data breach," which the plaintiff had not shown to be certainly impending).

In any event, by failing to respond specifically to this argument in her opposition, Plaintiff has forfeited the point. ECF No. 18 at 8–9 (addressing the standing argument solely in the context of her request for

injunctive relief, section header notwithstanding); *Platt v. CitiMortgage, Inc.*, 632 F. App'x 294, 295 (7th Cir. 2016) (“[A] party may waive an argument ‘by not responding to alleged deficiencies in a motion to dismiss’” (quoting *Alioto v. Town of Lisbon*, 651 F.3d 715, 721 (7th Cir. 2011))). Accordingly, the Court will grant Defendant’s motion to dismiss to the extent that it seeks dismissal of Plaintiff’s claim for declaratory relief. ECF No. 1 at 42–43; see *Ramsay*, 420 F. App'x at 588 (“If plaintiffs indeed lack standing, . . . then dismissal must be *without* prejudice” (citing *Steel Co.*, 523 U.S. 83)).

4.2 Failure to State Claims Upon Which Relief Can Be Granted

4.2.1 Cognizable Loss or Damages

Defendant argues that Plaintiff has failed to plausibly plead cognizable loss or damages, which “is an indispensable element of Plaintiff’s claims for (1) negligence; (2) negligence per se; (3) breach of fiduciary duty; (4) unjust enrichment; (5) breach of implied contract; and (6) violations of the [WDTPA].” ECF No. 15 at 9 (collecting cases).⁴ Defendant specifically challenges Plaintiff’s reliance on “damage to and diminution in the value of her PII.” *Id.* (citing ECF No. 1 at 15). Defendant also argues that Plaintiff’s “individual experiences,” such as the alleged increase in spam and scam calls and emails, are not traceable to the data breach because Plaintiff’s “email address and phone number were not impacted” by the data breach. ECF No. 15 at 10.

⁴Plaintiff does not suggest that she does not need to plead cognizable loss or damages for each of these claims. The Court accordingly does not scrutinize Defendant’s assertion that cognizable loss or damage is an “indispensable element of” those claims. ECF No. 15 at 9.

The Court will begin with, and reject, the latter argument.⁵ Defendant's contention that Plaintiff's email address and phone number were not disclosed in the data breach is not supported by the complaint. While it is true that the Notice of Data Breach explicitly identified only Plaintiff's name and Social Security number as potentially impacted, ECF No. 1-1 at 2, the complaint also states that "Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when." ECF No. 1 at 9. In other words, the fact that Defendant confirmed that certain pieces of Plaintiff's PII/PHI were impacted by the breach does not foreclose the possibility that other pieces of her PII/PHI were also exposed. *See id.* at 14 ("Through its Data Breach, Defendant compromised *at least* Plaintiff's name and Social Security number." (emphasis added)).

The Court next addresses Defendant's challenge to Plaintiff's asserted "actual injury in the form of damages to and diminution in the value of her PII/PHI." ECF No. 1 at 15; ECF No. 15 at 9–10. Defendant argues that Plaintiff fails to "allege any facts regarding how the data breach diminished the value of her PII or that she intended to sell her own PII." ECF No. 15 at 9 (citing *Silha v. ACT, Inc.*, 807 F.3d 169, 172 (7th Cir. 2015)).

The Court agrees that the alleged diminution in value of Plaintiff's PII/PHI does not constitute a cognizable loss. To the extent that Plaintiff makes allegations on this topic, they are highly generalized. Plaintiff alleges that stolen PII/PHI is "one of the most valuable commodities on the criminal

⁵As an organizational matter, it is not clear why this argument appears in the 12(b)(6) portion of Defendant's brief; traceability is a component of standing, not an element of any of Plaintiff's causes of action. *Pit Row, Inc. v. Costco Wholesale Corp.*, 101 F.4th 493, 502 (7th Cir. 2024) (identifying traceability as an "element of standing").

information black market” and that it “trades on the black market for years,” ECF No. 1 at 16, but she does not plausibly plead that the PII/PHI’s presence on the dark web in fact diminishes its economic value elsewhere, nor that she can or would ever sell it herself. *See In re Practicefirst Data Breach Litig.*, No. 1:21-CV-00790(JLS/MJR), 2022 U.S. Dist. LEXIS 19272, at *24–25 (W.D.N.Y. Feb. 1, 2022) (“[P]laintiffs have failed to allege a concrete or actual injury based on a diminution in value of their PHI and PII as a result of the data breach. . . . [P]laintiffs do not allege that they attempted to sell their personal information and were forced to accept a decreased price, nor do they allege any details as to how their specific, personal information has been devalued because of the breach.” (citing *Wallace v. Health Quest Sys.*, 20 CV 545, 2021 U.S. Dist. LEXIS 54557 (S.D.N.Y. Mar. 22, 2012); *Pena v. British Airways, PLC (UK)*, 18-CV-6278, 2020 U.S. Dist. LEXIS (E.D.N.Y. Mar. 30, 2020); and *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017))); *see also McLaughlin v. Taylor Univ.*, No. 1:23-cv-00527-HAB-SLC, 2024 U.S. Dist. LEXIS 172249, at *10–11 (N.D. Ind. Sept. 23, 2024) (“[I]t is hard to see how the value of Plaintiffs’ PII has been diminished. Plaintiffs fail to ‘explain how the hackers’ possession of . . . information has diminished its value, nor d[o] [they] assert that [they] would ever actually sell [their] own personal information. . . . Instead, Plaintiffs rely on a litany of general allegations highlighting PII’s value on the black market . . . None of those allegations suggest that Plaintiffs’ PII lost value in legitimate markets.” (quoting *Khan v. Children’s Nat’l Health Sys.*, 188 F. Supp. 3d 524, 531 (D. Md. 2016))).

Nevertheless, the Court cannot agree with Defendant that Plaintiff fails to plausibly plead any cognizable loss or damages as required to state her claims for negligence, negligence per se, breach of fiduciary duty, unjust

enrichment, breach of implied contract, and violations of the WDTPA. Plaintiff has plausibly pleaded, for example, that she “has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft.” ECF No. 1 at 14. The Seventh Circuit has held in the data breach context that “the value of one’s own time needed to set things straight is a loss from an opportunity-cost perspective” which “can justify money damages.” *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir. 2018); *see also Reetz v. Advocate Aurora Health, Inc.*, 983 N.W.2d 669, ¶ 13 (Wis. Ct. App. 2022) (“Reetz’s damages do not arise only from the overdraft fees, but [also] from allegations of ‘time spent dealing with fraud attempts [and] the threat of future identity theft.’” (quoting *Yvonne Mart Fox v. Iowa Health Sys.*, 399 F. Supp 3d 780, 790 (W.D. Wis. 2019))). Defendant does not suggest otherwise. Accordingly, Defendant’s motion to dismiss Plaintiff’s claims for negligence, negligence per se, breach of fiduciary duty, unjust enrichment, breach of implied contract, and violations of the WDTPA is denied to the extent that it is grounded in this cognizable loss argument.

4.2.2 Negligence Claim

Defendant also argues that Plaintiff’s negligence claim is subject to dismissal because Plaintiff merely “recites the legal elements of a negligence claim” without pleading specific, non-conclusory facts. ECF No. 15 at 10–11. Defendant also contends that Plaintiff’s negligence claim should be dismissed because Plaintiff has failed to plead what, specifically, made Defendant’s data security measures unreasonable. *Id.* at 11 (“Plaintiff refers to generalized industry standards, but does not even state what ‘industry standard’ she is relying on to demonstrate that the cybercriminal’s

attack could have been or should have been prevented.”). The Court disagrees.

“Under Wisconsin law, a claim for negligence requires the plaintiff to allege: (1) a breach of (2) a duty owed (3) that results in (4) an injury or injuries, or damages.” *Harbaugh v. Hertrampf*, No. 24-CV-850, 2024 U.S. Dist. LEXIS 212837, at *4 (E.D. Wis. Nov. 22, 2024) (citing *Paul v. Skemp*, 625 N.W.2d 860, 865 (Wis. 2001)).⁶

The Court has already concluded *supra* Section 4.2.1 that Plaintiff sufficiently pleads injury or damages. The Court is also satisfied that she sufficiently pleads the remaining elements of a negligence claim under Wisconsin law. As to duty, Plaintiff pleads that Defendant had “a duty to timely and accurately disclose . . . the scope, nature, and occurrence of the Data Breach,” a “duty to use reasonable security measures,” and “to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain.” ECF No. 1 at 26–27. She alleges that Defendant owed her and the other putative class members a duty of care “because it was foreseeable that Defendant’s failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach.” *Id.* at 26.

Defendant complains that Plaintiff isn’t specific enough about what “standard” Defendant’s data security needed to meet, ECF No. 15 at 11, but the Court cannot agree. Plaintiff specifically sets forth in her complaint the various FTC data protection guidelines, cybersecurity frameworks, and

⁶The parties do not dispute that Wisconsin law applies. ECF No. 15 at 10; ECF No. 18 at 11. Seeing no clear reason to disagree, the Court will assume the same. *See Allstate Indem. Co. v. ADT LLC*, 110 F. Supp. 3d 856, 860 (N.D. Ill. 2015) (citing *Harter v. Iowa Grain Co.*, 220 F.3d 544, 559 n.13 (7th Cir. 2000)).

HIPAA provisions that she contends Defendant should have, but failed, to adhere to. ECF No. 1 at 18–23. The Court sees no reason why more should be required of Plaintiff at this stage. *Cf. Reetz*, 983 N.W.2d, ¶¶ 11, 17 (denying motion to dismiss Wisconsin law negligence claim where the plaintiff pleaded that the defendant “had a duty of care to safeguard the PII within its control because it was foreseeable that cybercriminals would attempt to access the PII”).

As to breach, Plaintiff pleads that Defendant maintained “inadequate security practices,” failed to prevent the data breach and stop cybercriminals from accessing the PII/PHI, “kept the [c]lass in the dark” by failing to timely notify it of the breach, and “failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.” ECF No. 1 at 8–9. These allegations go beyond a bare recitation of the element of breach by specifying *how* Defendant allegedly breached its duty or duties to Plaintiff.

Lastly, Plaintiff has sufficiently pleaded causation. She plausibly alleges that Defendant’s cybersecurity failures caused her injuries. Given Defendant’s concession that Plaintiff’s name and Social Security number were exposed, ECF No. 1-1 at 2, and Plaintiff’s allegation that “3 TB” (terabytes) of PII/PHI stolen from Defendant’s network have already been published on the dark web, *id.* at 10–11, it is entirely plausible that Defendant’s alleged breaches caused Plaintiff’s injuries. If Defendant truly did not believe that to be a possible outcome of its failure to prevent the data breach, then it likely would not have “encourage[d]” Plaintiff and the other putative class members to “enroll in the credit monitoring and identity protection services,” among “additional steps.” ECF No. 1-1 at 2. *See Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *36 (noting as relevant to

causation element of negligence claim that the defendant “sent [the plaintiffs] letters encouraging them ‘to remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring free credit reports for suspicious activity, and to detect errors’”).

In light of the foregoing, Defendant’s motion to dismiss Plaintiff’s negligence claim for failure to state a claim is denied.

4.2.3 Negligence *Per Se* Claim

Defendant also moves the Court to dismiss Plaintiff’s negligence per se claim, which is premised on alleged violations of both the FTC Act, 15 U.S.C. § 45 (“FTCA”), and HIPAA. ECF No. 15 at 11–13; ECF No. 1 at 29–30.

“Negligence *per se* ordinarily refers to a form of ordinary negligence that results from violation of a statute.” *D.L. v. Huebner*, 329 N.W.2d 890, 917 (Wis. 1983); *see also Taft v. Derricks*, 613 N.W.2d 190, ¶ 11 (Wis. Ct. App. 2000) (“Negligence per se arises when the legislature defines a person’s standard of care in specific instances.”). But not just any statute; negligence per se exists “only when the defendant has violated a ‘safety statute,’” as opposed to a “more general regulatory measure[.]” *Cooper v. Eagle River Mem. Hosp., Inc.*, 270 F.3d 456, 460 (7th Cir. 2001); *see also Grube v. Daun*, 563 N.W.2d 523, 528 (Wis. 1997) (“Safety statutes are those legislative enactments that are designed to protect a certain class of persons from a particular type of harm. . . . A statute is not a safety statute if the legislature merely intended to protect the general public.” (citing *Bennett v. Larsen Co.*, 348 N.W.2d 540, 548 (Wis. 1984); *Walker v. Bignell*, 301 N.W.2d 447, 454 (Wis. 1981); and *In re Estate of Drab*, 422 N.W.2d 144, 145 (Wis. Ct. App. 1988))).⁷

⁷Defendant does not contend that the statutes upon which Plaintiff premises her negligence per se claim are not safety statutes, so the Court assumes

“The violation of the statute is the deviation from the standard of care and supplies” the “breach” element of the cause of action. *D.L.*, 329 N.W.2d at 917 (citing *McAleavy v. Lowe*, 49 N.W.2d 487, 494 (Wis. 1951)).

“Wisconsin courts have set limitations on whether a statutory violation will constitute negligence per se.” *Taft*, 613 N.W.2d, ¶ 12. For a statutory violation to constitute negligence per se, the following three circumstances must be met:

(1) the harm inflicted was the type the statute was designed to prevent; (2) the person injured was within the class of persons sought to be protected; and (3) there is some expression of legislative intent that the statute become a basis for the imposition of civil liability.

Id. (quoting *Antwaun A. v. Heritage Mut. Ins. Co.*, 596 N.W.2d 456, ¶ 41 (Wis. 1999)). With respect to the third element, “the legislation must evince a clear and unambiguous legislative desire to establish civil liability.” *Cooper*, 270 F.3d at 460 (citing *Leahy v. Kenosha Mem. Hosp.*, 348 N.W.2d 607, 612 (Wis. Ct. App. 1984)). “All three questions must be answered affirmatively before the statutory violation will constitute negligence per se.” *Taft*, 613 N.W.2d, ¶ 12 (citing *Antwaun A.*, 596 N.W.2d, ¶ 41).

Defendant challenges Plaintiff’s attempt to premise her negligence per se claim on violations of the FTCA and HIPAA. ECF No. 15 at 12. According to Defendant, alleged FTCA and/or HIPAA violations cannot constitute negligence per se under Wisconsin law because neither the FTCA nor HIPAA create “a private right of action.” *Id.* at 12–13 (citing *Merriam v. GC Servs.*, No. 1:18cv80, 2018 U.S. Dist. LEXIS 103636, at *2 (N.D. Ind. June 21, 2018); *Holloway v. Bristol-Myers Corp.*, 485 F.2d 986, 989 (D.C. Cir. 1973);

for purposes of the instant motion that they are safety statutes and discusses that aspect of the analysis no further.

and *Wall v. Pahl*, 886 N.W.2d 373, ¶ 25 (Wis. Ct. App. 2016)); ECF No. 20 at 10 (same). But that argument appears to mischaracterize the third required element for a statutory violation to constitute negligence per se under Wisconsin law; there must be “some expression of legislative intent that the statute become a basis for the imposition of civil liability,” *Taft*, 613 N.W.2d, ¶ 12, but that is not necessarily to say that the statute must create a *private* cause of action. *Dusterhoff*, 2024 U.S. Dist. LEXIS 170993, at *41 (“While [the defendant] is correct that neither HIPAA nor Section 5 [of the FTCA] creates a private right of action, that is not necessarily required for a claim of negligence per se. . . . Both HIPAA and Section 5 [of the FTCA] authorize the federal government to impose civil liability for violations akin to those [the defendant] is accused of committing.” (citing *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015) and 45 C.F.R. § 160.402)); see also *Troth v. Warfield*, 495 F. Supp. 3d 729, 737 (N.D. Ind. 2020) (applying Indiana law) (“The doctrine of negligence *per se*, however, is separate from whether the statute provides a private cause of action.”). Certainly, a statute’s creation of a private cause of action would constitute “expression of legislative intent that the statute become a basis for the imposition of civil liability,” *Taft*, 613 N.W.2d, ¶ 12 (citation omitted), but it does not appear that that is the *only* circumstance in which the third element is met. See *Walker*, 301 N.W.2d at 455–56 (“[T]here does not emerge any discernible legislative intent to impose civil liability under Chapter 70 However, we believe the requisite intent [to impose civil liability] may be supplied by necessary implication from the language of the statute. The language added by the 1949 amendment is such a clear expression of concern for the safety of highway users, committed so plainly to the responsibility of the public highway authorities, that we conclude that the municipal bodies so charged

are exposed to civil liability for their failure to do that with which they are charged. We conclude, therefore, that [the statute] created a basis for civil liability in favor of highway users.”). The cases upon which Defendant relies do not say otherwise; neither *Merriam* nor *Holloway* even involve negligence per se claims.

Defendant also challenges Plaintiff’s attempt to premise her negligence per se claim on HIPAA because “Plaintiff does not allege that Defendant is a covered entity, and in the notice of data breach . . . , the information potentially impacted did not include any of Plaintiff’s health information.” ECF No. 15 at 13 (citing ECF No. 1-1).

The Court has, albeit in a slightly different context, already rejected the latter argument, *see supra* Section 4.2.1. Plaintiff plausibly alleges that although she only received confirmation regarding the exposure of her name and Social Security number, other information—including medical and health insurance information—was also compromised. ECF No. 1 at 7. Again, the fact that Defendant was able to confirm that Plaintiff’s name and Social Security number were compromised does not mean that other pieces of her PII/PHI—including medical and health insurance information—were not also compromised. *See id.* at 14 (“Through its Data Breach, Defendant compromised *at least* Plaintiff’s name and Social Security number.” (emphasis added)).

With respect to the first argument, Defendant is correct that Plaintiff fails to specifically allege that Defendant is a “covered entity” under HIPAA. ECF No. 15 at 13. Plaintiff’s response to this argument is not particularly compelling. ECF No. 18 at 13 (asserting only that Plaintiff “itself reported to the Massachusetts Attorney General that PHI protected under HIPAA was stolen”).

“HIPAA’s privacy protections restrict the use and disclosure of protected health information by *covered entities*” *Long v. Wondra*, No. 12-cv-647-wmc, 2013 U.S. Dist. LEXIS 192902, at *15 (W.D. Wis. Sept. 16, 2013) (citing 42 U.S.C. §§ 1320d-1, 1320d-2 and 45 C.F.R. § 164.502 (emphasis added)). Under HIPAA, a “covered entity” means “[a] health plan,” “[a] health care clearinghouse,” or “[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.” 45 C.F.R. § 160.103. Nothing in Plaintiff’s complaint suggests that Defendant falls within that definition, and if it is not a “covered entity” subject to HIPAA’s mandates, it necessarily could not violate HIPAA. Accordingly, the Court ultimately agrees that Plaintiff’s negligence per se claim as premised on a HIPAA violation must be dismissed. While the Court does not anticipate that Plaintiff will be able to remedy that deficiency via amendment, the Court will, out of an abundance of caution, order that the dismissal operate without prejudice. *See Circle Block Partners, LLC v. Fireman’s Fund Ins. Co.*, 44 F.4th 1014, 1023 (7th Cir. 2022) (citing *Runnion ex rel. Runnion v. Girl Scouts of Greater Chi. & Nw. Ind.*, 786 F.3d 510, 519 (7th Cir. 2015) and *Zimmerman v. Bornick*, 25 F.4th 491, 494 (7th Cir. 2022)).

For all these reasons, Plaintiff’s negligence per se claim is dismissed without prejudice to the extent that it is premised on a HIPAA violation. Plaintiff’s negligence per se claim as premised on a FTCA violation may proceed. The Court acknowledges the *Dusterhoft* court’s concern as to whether a FTCA violation can, in fact, “form the basis for negligence per se” under Wisconsin law. 2024 U.S. Dist. LEXIS 170993, at *42. But the burden of proffering sufficient on-point argument and authority to support the dismissal of that claim was on Defendant, and Defendant did not meet

it. That conclusion finds some support in persuasive authority, albeit under the application of other states' laws. *See, e.g., In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1327–28 (N.D. Ga. 2019) (denying motion to dismiss negligence per se claim under Georgia law based on violation of the FTCA); *Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7:13-cv-00360-JCT, 2014 U.S. Dist. LEXIS 19953, at *34–41 (W.D. Va. Feb. 12, 2014) (same under Virginia law); *McLaughlin*, 2024 U.S. Dist. LEXIS, at *18–20 (same under Indiana law); *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760–61 (C.D. Ill. 2020) (same under Illinois law).

4.2.4 Breach of Implied Contract Claim

Defendant next moves the Court to dismiss Plaintiff's breach of implied contract claim. ECF No. 15 at 13–14. Defendant argues that "Plaintiff's breach of implied contract [claim] fails because Plaintiff does not plausibly allege the existence of an implied contract to prevent cyberattacks, let alone a breach of some undefined implied contract." *Id.* at 13. "[N]oticeably absent from the Complaint," Defendant argues, "is any allegation about what Defendant implicitly promised to do to prevent this data breach, or what benefit was conferred on Defendant." *Id.* at 14.

In opposition, Plaintiff argues that "[b]y soliciting and collecting employee data, [Defendant] impliedly promised to safeguard it, creating an enforceable obligation." ECF No. 18 at 14 (citing *Linman v. Marten Transp., Ltd.*, 22-cv-204-jdp, 2023 U.S. Dist. LEXIS 45661, at *13 (W.D. Wis. Mar. 17, 2023)).

Wisconsin recognizes both contracts implied in fact and implied in law. *Lindquist Ford, Inc. v. Middleton Motors, Inc.*, 557 F.3d 469, 480–81 (7th Cir. 2009). "[A] 'quasi-contract or contract implied-in-law differs markedly from a contract implied-in-fact.'" *Id.* at 480 (quoting *Stromsted v. St. Michael*

Hosp. of Franciscan Sisters, 299 N.W.2d 226, 228 n.1 (Wis. 1980)). “[A]n implied-in-fact contract is governed by general contract principles,” but an implied-in-law contract is not. *Id.* at 481. A contract that is “‘implied in law’ . . . is an obligation that is created by the law without regard to expression of assent by either words or acts.” 1 CORBIN ON CONTRACTS § 1.20 (2024).

Under which version of the claim Plaintiff intended to proceed is not clear. Defendant’s motion to dismiss the breach of implied contract claim cites to *Reetz*, a case discussing breach of an implied-in-law contract. ECF No. 15 at 13 (citing 983 N.W.2d, ¶ 28). Plaintiff’s response also relies on the standard set forth in *Reetz*, ECF No. 18 at 14, which would suggest that its breach of implied contract claim is one for breach of implied-in-law contract. But, as the court acknowledged in *Reetz*, “an implied [in law] contract is an awkward application to the facts of this case” 983 N.W.2d, ¶ 29. Confusingly, Plaintiff goes on to rely on cases involving implied-in-fact contract claims, contending that, as in those cases, “Plaintiff sufficiently alleges a contractual relationship,” which is not an element of an implied-in-law contract claim. ECF No. 18 at 14–15 (citing *Hall*, 2023 U.S. Dist. LEXIS 83438, at *16–17; *Brahm v. Hosp. Sisters Health Sys.*, 23-cv-444-wmc, 2024 U.S. Dist. LEXIS 114827, at *12 (W.D. Wis. June 28, 2024); and *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 821 (E.D. Ky. 2019)); 1-1 MURRAY ON CONTRACTS § 21 (2024) (noting that implied-in-law contracts involve “no real promise and none of the other elements of a real contract”). In other words, Plaintiff appears to be conflating two types of implied contract claims.⁸

⁸In Plaintiff’s defense, courts confuse the matter, too. *Lindquist Ford*, 557 F.3d at 480–81; 1-1 MURRAY ON CONTRACTS § 21 (2024) (“The ‘implied contract’ term can be misleading . . .”).

To the extent that it was intended to be an implied-in-law claim, the claim is essentially duplicative of Plaintiff's unjust enrichment claim. *See infra* Section 4.2.6. The elements for breach of an implied-in-law contract claim and an unjust enrichment claim are the same under Wisconsin law. *See W.H. Fuller Co. v. Seater*, 595 N.W.2d 96, 99 (Wis. Ct. App. 1999) ("A contract implied in law consists of three elements: '(1) a benefit conferred upon the defendant by the plaintiff; (2) knowledge or appreciation of the benefit by the defendant; and (3) acceptance and retention by the defendant of such benefit under such circumstances that it would be inequitable for him or her to retain it without paying the value thereof.'" (quoting Wis. JI—Civil 3028 and citing *Watts v. Watts*, 405 N.W.2d 303, 313 (Wis. 1987))); *Nationwide Advantage Mortg. Co. v. GSF Mortg. Corp.*, No. 13-cv-1420, 2015 U.S. Dist. LEXIS 130190, at *14 (E.D. Wis. Sept. 25, 2015) ("Under Wisconsin law, an unjust enrichment claim consists of the following elements: (1) a benefit conferred on defendant, (2) defendant's knowledge of and appreciation of that benefit, and (3) inequity that results from defendant's retention of that benefit." (citing *Beer Capitol Distrib., Inc. v. Guinness Bass Imp. Co.*, 290 F.3d 877, 881 (7th Cir. 2002))). "[A] contract implied in law necessarily involves recovery through unjust enrichment" *W.H. Fuller Co.*, 595 N.W.2d at 99. Accordingly, the Court will limit its analysis in this section to the theory of implied-in-fact contracts.

As earlier noted, an implied-in-fact contract is "governed by general contract principles." *Lindquist Ford*, 557 F.3d at 481. It "requires, the same as an express contract, the element of mutual meeting of minds and of intention to contract." *Id.* (quoting *Theuerkauf v. Sutton*, 306 N.W.2d 651, 657 (Wis. 1981)). "[A] contract is implied in fact where the intention as to it is not manifested by direct or explicit words between the parties, but is to be

gathered by implication or proper deduction from the conduct of the parties, language used or things done by them, or other pertinent circumstances" *Theuerkauf*, 306 N.W.2d at 658 (quoting *Erickson v. Goodell Oil Co., Inc.*, 180 N.W.2d 798, 800 (Mich. 1970)).

Plaintiff's allegations are vague, obscure, and confusing with respect to this claim. According to her complaint, Plaintiff does not know whether she "directly contracted with Defendant" or if she was instead a "third-party beneficiar[y] of contracts with Defendant." ECF No. 1 at 31. She admits that she does not even know "precisely how and why Defendant obtained . . . her PII/PHI." *Id.* at 13. Further confusing matters, the complaint at one point states that Plaintiff was required to provide her PII/PHI as a condition of her employment with her non-party employer, *id.*, but it elsewhere states that she was required to provide her PII/PHI "as a condition of receiving services provided by Defendant," *id.* at 31. The complaint also states that Plaintiff "paid Defendant" "for adequate cybersecurity measures," *id.*, which is difficult, if not impossible, to reconcile with Plaintiff's allegations that she does not know "precisely how and why Defendant obtained . . . her PII/PHI" and does not know whether she "directly contracted with Defendant." *Id.* at 13, 31. At bottom, her allegations as to this claim are indicative of a planned fishing expedition.

Given the confusing, obscure, and contradictory nature of her factual allegations as relevant to this claim, the Court cannot conclude that Plaintiff has plausibly pleaded that the parties had any "mutual meeting of the minds and of intention to contract." *Lindquist Ford*, 557 F.3d at 481 (citation omitted). "[E]ven an implied [in fact] contract must arise under circumstances which show a mutual intention to contract. The minds of the parties must meet on the same thing." *Theuerkauf*, 306 N.W.2d at 657

(quoting *Kramer v. Hayward*, 203 N.W.2d 871, 873–74 (Wis. 1973)). Plaintiff's complaint does not plausibly allege that "essential element" of a breach of implied-in-fact contract claim. *Id.* (quoting *Kramer*, 203 N.W.2d at 874).

The cases on which Plaintiff relies in her opposition do not convince the Court otherwise. Unlike the plaintiffs in those cases, she has not alleged that she was herself either a client, employee, or patient of the defendant. *Hall*, 2023 U.S. Dist. LEXIS 83438, at *14–17 (denying motion to dismiss breach of implied contract claim where complaint plausibly alleged that the plaintiff was an employee of the defendant's subsidiary or predecessor and that he was required to provide his PII to the defendant company as a condition of obtaining and maintaining employment); *Brahm*, 2024 U.S. Dist. LEXIS 114827, at *3, *5–6 (denying motion to dismiss breach of implied contract claim where the plaintiff was a patient of the defendant hospital system and plausibly alleged that the defendant made promises regarding access to patients' computers); *McKenzie*, 369 F. Supp. 3d at 821 (denying motion to dismiss breach of implied contract claim where plaintiff employee claimed that defendant employer promised in employment agreement to secure information). Unlike the plaintiffs in those cases, in which the breach of implied contract claims were allowed to proceed, Plaintiff appears to have been a step removed from the arrangement in which her PII/PHI made its way onto Defendant's network.

Plaintiff's reliance on a third-party beneficiary theory does not save her claim. For one, her complaint's invocation of this theory is little more than a bare recitation of the key buzzwords associated with the theory. See ECF No. 1 at 31. Those bald allegations fall short. "To be a third-party beneficiary of a contract, the contract must intentionally be entered into for the direct benefit of the third party." *Grams v. Milk Prods., Inc.*, 685 N.W.2d

172, ¶ 10 (Wis. 2004) (citing *Mercado v. Mitchell*, 264 N.W.2d 532, 538 (Wis. 1978)); see also *Schilling by Foy v. Emps. Mut. Cas. Co.*, 596 N.W.2d 776, 780 (Wis. Ct. App. 1997) (“The person claiming to be a third party beneficiary must show that the contract was entered into by the parties to the contract directly and primarily for the benefit of the third party.” (citing *Goossen v. Est. of Standaert*, 525 N.W.2d 314, 319 (Wis. Ct. App. 1994))). “The benefit must be more than incidental.” *Grams*, 685 N.W.2d, ¶ 10 (citing *Krawczyk v. Bank of Sun Prairie*, 496 N.W.2d 218, 220 (Wis. Ct. App. 1993)). Further, “[t]he contract must indicate that the third party either was specifically intended by the contracting parties to benefit from the contract, or is a member of the class the contracting parties intended to benefit.” *Schilling*, 596 N.W.2d at 780 (citing *Goossen*, 525 N.W.2d at 319). Plaintiff’s complaint does not plausibly allege nor allow for the inference that her employer intentionally entered into a contract with Defendant specifically “for the direct benefit” of Plaintiff. *Grams*, 685 N.W.2d, ¶ 10. The complaint does not clarify what the nature of any such contract between Plaintiff’s employer and Defendant would have been, let alone assert that it was entered into primarily for Plaintiff’s benefit and that it indicated the same. Further, Plaintiff’s response in opposition to the motion to dismiss her breach of implied contract claim does not clarify matters, as it does not address the third-party beneficiary theory whatsoever, despite Defendant’s reference to it as one of the “medley of allegations” included as to that claim. ECF No. 15 at 13; ECF No. 18 at 14–15.

For all these reasons, Plaintiff’s breach of implied contract claim will be dismissed. However, because the Court cannot necessarily conclude that amendment as to this claim would be futile, the dismissal of this claim will

operate without prejudice. *See Circle Block Partners*, 44 F.4th at 1023 (citing *Runnion*, 786 F.3d at 519 and *Zimmerman*, 25 F.4th at 494).

4.2.5 Wis. Stat. § 995.50(2) Claim

Defendant next moves the Court to dismiss Plaintiff's claim for invasion of privacy under Wis. Stat. § 995.50(2). ECF No. 15 at 14–16. Plaintiff claims that Defendant violated both subsection (am)(1) (intrusion upon private place) and subsection (am)(3) (public disclosure of private information). ECF No. 1 at 33; ECF No. 18 at 15. Defendant contends that “[b]oth theories fail.” ECF No. 15 at 14. The Court agrees.

4.2.5.1 Intrusion Upon Private Place

The Court begins with Defendant's challenge to Plaintiff's claim under subsection (am)(1). Wis. Stat. § 995.50(2)(am)(1) provides that “invasion of privacy” means “[i]ntrusion upon the privacy of another of a nature highly offensive to a reasonable person . . . in a place that a reasonable person would consider private, or in a manner that is actionable for trespass.” Defendant argues that “the plain meaning of ‘a place’ is geographical,” and that Plaintiff fails to allege any intrusion or trespass upon a geographical place. ECF No. 15 at 15 (quoting *Hillman v. Columbia County*, 474 N.W.2d 913, 919 (Wis. Ct. App. 1991)) (internal quotation marks omitted). Plaintiff disputes that Wisconsin law “limit[s] privacy intrusions to physical spaces,” although she cites to no authority in support of this position. ECF No. 18 at 15.

By disputing Defendant's argument without any citation to authority, Plaintiff has forfeited the point. *Beverly v. Abbott Lab'ys*, 817 F.3d 328, 334 (7th Cir. 2016) (citing *United States v. Berkowitz*, 927 F.2d 1376, 1384 (7th Cir. 1991)). In any event, Wisconsin caselaw supports Defendant's argument. In *Uebelacker v. Rock Energy Cooperative*, the Wisconsin Court of

Appeals, relying on *Hillman*, rejected a plaintiff's claim that her employer violated her right to privacy under § 995.50(2)(am)(1) when its IT manager viewed her Facebook Messenger conversation. 2025 Wisc. App. LEXIS 166, ¶¶ 12–14 (Wis. Ct. App. 2025) (citing *Hillman*, 474 N.W.2d 913); *Hillman*, 474 N.W.2d at 919 (“We believe that the plain meaning of ‘a place’ is geographical. It does not include a file of medical records.”); *see also Buckeridge v. Univ. of Wis. Hosp. & Clinics Auth. UW Health*, 932 N.W.2d 185, ¶¶ 12–13 (Wis. Ct. App. 2019) (concluding for purposes of violation of privacy claim that “medical records stored on a computer system” do not constitute a “place” under the statute). Because Plaintiff has not plausibly alleged any intrusion into a protected “place” as contemplated by § 995.50(2)(am)(1), her invasion of privacy claim fails to the extent that it is premised on that subsection. And since amendment as to this claim would be futile, the dismissal will operate with prejudice. *See Circle Block Partners*, 44 F.4th at 1023 (citing *Runnion*, 786 F.3d at 519 and *Zimmerman*, 25 F.4th at 494).

4.2.5.2 Public Disclosure of Private Information

The Court next addresses subsection (am)(3), which provides that “invasion of privacy” means “[p]ublicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed.” Wis. Stat. § 995.50(2)(am)(3). A claim under this subsection involves four elements:

- (1) a public disclosure of facts regarding the plaintiff; (2) the facts disclosed must be private facts; (3) the private matter made public must be one which would be highly offensive to a reasonable person of ordinary sensibilities; and (4) the

defendant must act either unreasonably or recklessly as to whether there was a legitimate public interest in the matter, or with actual knowledge that none existed.

Hillman, 474 N.W.2d at 919–20 (citing *Zinda v. La. Pac. Corp.*, 440 N.W.2d 548, 555 (Wis. 1989)).

Defendant contends that, although the statute’s text does not itself so state, this claim is categorized as an intentional tort, and that Plaintiff’s failure to allege that Defendant *intentionally* disclosed Plaintiff’s PII/PHI dooms the claim. ECF No. 15 at 15–16 (citing *Fox*, 399 F. Supp. 3d at 796). Plaintiff disputes that § 955.50(2)(am)(3) requires an intentional disclosure. ECF No. 18 at 16 (citing *Linman*, 2023 U.S. Dist. LEXIS 45661, at *16).

In 2019, Judge James Peterson in the Western District of Wisconsin acknowledged in *Fox* that Wis. Stat. § 955.50(2)(am)(3) did “not specify whether the first element of this claim requires intentional disclosure by the defendant.” 399 F. Supp. 3d at 796. “But,” the court reasoned, Wisconsin law “categorizes invasion of privacy as an intentional tort . . . [a]nd courts that have considered similar claims in other jurisdictions have held that intentional action is required.” *Id.* (collecting cases in footnote).

In 2022, the Wisconsin Court of Appeals in *Reetz* agreed with Judge Peterson and concluded that “the publicity of private facts cause of action requires intentional conduct” 983 N.W.2d, ¶ 19 (rejecting the plaintiff’s contention that “intentional conduct is not required and that invasion of privacy is not an intentional tort” and acknowledging that the issue was one of “first impression” for Wisconsin courts (citing *Fox*, 399 F. Supp. 3d at 796–97)).

Plaintiff’s reliance on *Linman* is utterly unavailing; the court in *Linman* did not even address a claim under (am)(3). 2023 U.S. Dist. LEXIS

45661, at *16–17 (evaluating claim under (am)(1)). The Wisconsin Court of Appeals in *Reetz* could not have been clearer: a claim under § 955.50(2)(am)(3) “requires intentional conduct.” 983 N.W.2d, ¶ 19. This Court is bound by the state court’s interpretation of its own law. *Leonard v. Warden, Dodge Corr. Inst.*, 631 F. Supp. 1403, 1406 (E.D. Wis. 1986) (citation omitted); *see also Schlesinger v. Councilman*, 420 U.S. 738, 755 (1975) (“State courts . . . alone can define and interpret state law.”). Plaintiff concedes that she does not allege that Defendant intentionally disclosed her PII/PHI. *See* ECF No. 18 at 16. Her claim under Wis. Stat. § 955.50(2)(am)(3) must accordingly be dismissed. However, because the Court cannot necessarily conclude that amendment as to this claim would be futile, the dismissal of this claim will operate without prejudice. *See Circle Block Partners*, 44 F.4th at 1023 (citing *Runnion*, 786 F.3d at 519 and *Zimmerman*, 25 F.4th at 494).

4.2.6 Unjust Enrichment Claim

Defendant also moves the Court to dismiss Plaintiff’s unjust enrichment claim, which is pleaded in the alternative to her breach of implied contract claim. ECF No. 15 at 16–17; ECF No. 1 at 35–37.⁹

The elements of an unjust enrichment claim under Wisconsin law are: “(1) a benefit conferred upon the defendant by the plaintiff; (2) knowledge or appreciation of the benefit by the defendant; and (3) acceptance or retention by the defendant of such benefit under such circumstances that it would be inequitable for [the defendant] to retain it without paying the value thereof.” *Admiral Ins. Co. v. Paper Converting Mach. Co.*, 811 N.W.2d 351, ¶ 46 n.16 (Wis. 2012)) (citing Wis. JI—Civil 3028).

⁹ “[P]laintiffs are allowed to plead contract and unjust enrichment claims in the alternative.” *Fox*, 399 F. Supp. 3d at 803 (citing *Cromeens, Holloman, Sibert, Inc. v. AB Volvo*, 349 F.3d 376, 397 (7th Cir. 2003)).

Defendant takes issue solely with the first element, *see* ECF No. 15 at 16–17, so the Court elaborates on that element and addresses the others no further. For purposes of an unjust enrichment claim under Wisconsin law, the benefit conferred must be an “economic” one. *Larson v. Castle at the Bay, LLC*, 922 N.W.2d 321, ¶ 20 (Wis. Ct. App. 2018) (citing *Sands v. Menard*, 904 N.W.2d 789, ¶ 30 (Wis. 2017)); *see also* *Reetz*, 983 N.W.2d, ¶ 29 (“Unjust enrichment generally [involves] . . . a monetary benefit conferred upon a defendant . . .”).

Plaintiff’s unjust enrichment claim is premised on two alleged benefits to Defendant. The first is her PII/PHI itself because Defendant “us[ed] the[] PII/PHI to facilitate its business operations.” ECF No. 1 at 36; *id.* at 13 (“As a condition of her employment, Plaintiff (or her third-party agent) provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its business.”). The second is the money that either Plaintiff or Plaintiff’s third-party agent paid Defendant for Defendant’s services. *Id.* at 36, 14 (“Plaintiff reasonably understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of PII/PHI.”).

Defendant does not argue that Plaintiff or her third-party agent having paid Defendant for services, including information protection/cybersecurity, cannot meet the first element. The Court therefore assumes that this counts as an economic benefit for purposes of an unjust enrichment claim.¹⁰ *See, e.g., Baldwin v. Nat’l W. Life Ins. Co.*, No. 2:21-CV-

¹⁰The Court accordingly does not at this juncture delve into any issue with the potentially indirect nature of payment from Plaintiff’s employer to Defendant. *Compare Crumble v. Johnson*, 932 N.W.2d 193, ¶ 17 (Wis. Ct. App. 2019) (Table) (“[A] court may find unjust enrichment when a benefit is provided to the defendant by a third party.”), *with Weaver v. Champion Petfoods USA Inc.*, No. 18-CV-1996-JPS,

04066-WJE, 2021 U.S. Dist. LEXIS 175229, at *24 (W.D. Mo. Sept. 15, 2021) (“Courts within the Eighth Circuit have . . . allowed unjust enrichment claims for stolen PII when the plaintiff provided payment based on an understanding that their PII would be secure.” (citing *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014))).

The Court accordingly moves on to the other asserted benefit, the legal cognizability of which Defendant *does* challenge: Defendant’s alleged use of Plaintiff’s PII to facilitate its business operations. Defendant argues that “Plaintiff fails to allege any factual details supporting how her PII was a monetary benefit conferred and unjustly retained by Defendant.” ECF No. 15 at 16 (footnote omitted) (citing *Johnson v. Nice Pak Prods., Inc.*, 736 F. Supp. 3d 639, 652 (S.D. Ind. 2024)). In response, Plaintiff argues that “[n]umerous courts have rejected [Defendant’s] argument that employees do not confer a benefit on their employer or their agent by supplying necessary data.” ECF No. 18 at 17–18 (collecting cases).

To the Court’s knowledge, no Wisconsin court has answered the question of whether the conferral of PII can itself constitute a benefit for purposes of unjust enrichment.¹¹ But it appears that courts applying the laws of other states have largely rejected unjust enrichment claims

2019 U.S. Dist. LEXIS 109550, at *18 (E.D. Wis. July 1, 2019) (“The conferral of the benefit must be directly from the plaintiff to the defendant” (citing *Loeb v. Champion Petfoods USA Inc.*, 359 F. Supp. 3d 597, 605 (E.D. Wis. 2019))).

¹¹The court in *Reetz* circled the issue but did not go so far as to enunciate a holding as to whether such a circumstance could meet the first element of an unjust enrichment claim as a matter of law. 983 N.W.2d, ¶ 29 (“To find that a benefit was conferred upon [the defendant] by [the plaintiff] would mean that it was to [the defendant’s] benefit for [the plaintiff] to provide her PII [T]hat benefit to [the defendant] . . . is not alleged in the complaint and is unclear from our review of the facts.”).

premised on this theory, particularly where, as here, the plaintiff's allegations as to the alleged benefit are extremely vague. *See Robinson v. Maintech Inc.*, No. 23-04458, 2024 U.S. Dist. LEXIS 229536, at *7–8 (D.N.J. Dec. 19, 2024) (“[T]he [c]omplaint alleges that [the defendant] ‘benefitted from receiving Plaintiff’s . . . PII.’ However, courts in this district have dismissed similar unjust enrichment claims based on ‘conferring’ PII.” (cleaned up) (citing *In re Am. Med. Collection Agency, Inc. v. Customer Data Sec. Breach Litig.*, No. 19-2904, 2021 U.S. Dist. LEXIS 240360, at *67 (D.N.J. Dec. 16, 2021))); *In re NCB Mgmt. Servs., Inc. v. Data Breach Litig.*, No. 23-1236, 2024 U.S. Dist. LEXIS 163260, at *27–29 (E.D. Pa. Sept. 11, 2014) (granting motion to dismiss unjust enrichment claim where plaintiffs failed to “plead that [the defendant] became enriched ‘specific to the PII’ such that it ‘reaped monetary benefits or otherwise profited’ from holding plaintiffs’ PII” (citing *In re Am. Fin. Res., Inc. Data Breach Litig.*, No. 222CV01757CAJSA, 2023 U.S. Dist. LEXIS 108411 (D.N.J. Mar. 29, 2023))); *Nice Pak Prods.*, 736 F. Supp. 3d at 652 (concluding that any benefit to the defendant from the plaintiff’s PII was merely “incidental” and that “[t]he PII is better understood as necessary to conduct business operations, not a good whose inherent value was extracted by [the] [d]efendants”); *Cahill v. Mem’l Heart Inst., LLC*, No. 1:23-cv-168, 2024 U.S. Dist. LEXIS 174634, at *35–37 (E.D. Tenn. Sept. 26, 2024) (rejecting the plaintiffs’ argument that their PII “has inherent value” such that they “‘conferred a monetary benefit on [the] [d]efendant’ by giving [the] [d]efendant their PII” and noting that the plaintiffs “d[id] not allege that [the] [d]efendant commoditized, gained monetary benefit, or otherwise profited from Plaintiffs’ PII, except to the extent that it allowed [the] [d]efendant to provide . . . services”); *Hall*, 2023 U.S. Dist. LEXIS 83438, at *18 (dismissing unjust enrichment claim on

motion to dismiss where plaintiff alleged that “the personal information [that he] gave to the [defendant] . . . can serve as the benefit conferred for purposes of this claim”).

The Court is inclined to agree with the reasoning in those cases. But even if it didn’t, Plaintiff’s pleading of this claim would in any event fail to meet the requirements of Rule 8. Plaintiff alleges that Defendant benefitted from using her PII to facilitate its business operations, but it is not at all clear how. Her complaint lacks any contextualizing information as to what role Plaintiff’s PII played in Defendant’s business operation and how Defendant’s retention of her PII benefitted Defendant in some measurable, economic sense. And while her complaint goes to great lengths to emphasize the value of stolen PII on the dark web, ECF No. 1 at 16, it does nothing to describe the economic value of the PII to Defendant’s business. In light of all the foregoing, the Court concludes that Plaintiff’s allegation that Defendant’s use of her PII to facilitate its business was itself an economic benefit to Defendant fails to state the first element of an unjust enrichment claim. Her unjust enrichment claim is accordingly dismissed with prejudice to the extent that it was premised on that benefit. To the extent that her unjust enrichment claim is premised on Defendant’s alleged receipt of payment, ECF No. 1 at 36, the claim may proceed.

4.2.7 Breach of Fiduciary Duty Claim

Defendant also contends that Plaintiff fails to state a claim for breach of fiduciary duty. ECF No. 15 at 17–19. Defendant disputes that the relationship between Plaintiff and Defendant alleged in the complaint—i.e., “Defendant’s connection to Plaintiff’s employer”—constitutes a fiduciary relationship. *Id.* at 17–18. Defendant also argues that Plaintiff fails to allege

that Defendant had a fiduciary duty specifically “to protect her PII.” *Id.* at 17 (citing *Berner Cheese Corp. v. Krug*, 752 N.W.2d 800, ¶ 40 (Wis. 2008)).

In response, Plaintiff disputes Defendant’s characterization of the alleged fiduciary relationship; she argues that she “does not assert a typical employment relationship but instead alleges that [Defendant], as the custodian of sensitive PII/PHI, created a special relationship of trust and reliance.” ECF No. 18 at 18 (“By assuming custody over Plaintiff’s PII/PHI and assuring its protection, [Defendant] undertook a fiduciary duty to safeguard the information.”). She also argues that “[w]hether a fiduciary duty exists is a fact-intensive inquiry that cannot be resolved at the motion to dismiss stage.” *Id.* at 19 (citing *Berner Cheese Corp.*, 752 N.W.2d, ¶ 25; *Quad/Graphics, Inc. v. One2One Commc’ns LLC*, No. 09-CV-99, 2012 U.S. Dist. LEXIS 89520, at *23 (E.D. Wis. June 21, 2012); and *Est. of Moore v. Jessy Dixon & Jessy Dixon Ministries*, No. 06-C-321, 2008 U.S. Dist. LEXIS 132707, at *30 (E.D. Wis. Sept. 26, 2008)).

“The elements of a claim for breach of fiduciary duty are: (1) the defendant owed the plaintiff a fiduciary duty; (2) the defendant breached that duty; and (3) the breach of duty caused the plaintiff’s damage.” *Berner Cheese Corp.*, 752 N.W.2d, ¶ 40 (citing *Reget v. Paige*, 626 N.W.2d 302, ¶ 12 (Wis. Ct. App. 2001)); see also *Zastrow v. Journal Commc’ns, Inc.*, 718 N.W.2d 51, ¶ 27 (Wis. 2006) (“[I]n any analysis of a claimed breach of fiduciary duty, there are two central questions to address: was the relationship a fiduciary relationship, and if so, what is the nature of the fiduciary duty that is at issue?” (citing *Promises Broken vs. Promises Betrayed: Metaphor, Analogy, and the New Fiduciary Principle*, 1993 U. ILL. L. REV. 897, 905)).

“A fiduciary relationship arises from a formal commitment to act for the benefit of another . . . or from special circumstances from which the law

will assume an obligation to act for another's benefit." *Doe 67C v. Archdiocese of Milwaukee*, 700 N.W.2d 180, ¶ 55 (Wis. 2005) (quoting *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Boeck*, 377 N.W.2d 605, 609 (Wis. 1985)). Examples of fiduciary relationships include "trustee to beneficiary, guardian to ward, agent to principal, [and] attorney to client." *Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *46 (quoting *Zastrow*, 718 N.W.2d at 59). "In determining whether a fiduciary relationship has arisen, courts consider a variety of factors, including whether there is dependence and inequality based on weakness of age or mental strength, lack of business intelligence, inferior knowledge of facts involved, or other conditions giving one side an advantage over the other." *Doe 67C*, 700 N.W.2d, ¶ 55 (citing *Prod. Credit Ass'n of Lancaster v. Croft*, 423 N.W.2d 544, 547 (Wis. Ct. App. 1988)). "Central to [fiduciary] relationships is a substantial degree of trust and authority exercised by the fiduciary over the affairs of the other party." *Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *46.

Plaintiff cites to no on-point authority suggesting that the relationship she describes—Defendant as "custodian of sensitive PII/PHI"—is anything more than an arms-length arrangement; she does not argue that any relevant factor, as set forth in *Doe 67C*, supports the finding of a fiduciary relationship. ECF No. 18 at 18. Meanwhile, the only Wisconsin case the Court has located addressing the issue in the context of a data breach "reject[ed] [the notion] that the website or privacy policy of [the defendant] creates a fiduciary duty . . . to the Plaintiffs' PII." *Schaefer v. Johnson Fin. Grp., Inc.*, No. 2023CV1483, 2024 Wisc. Cir. LEXIS 25, at *6 (Wis. Cir. Ct. May 6, 2024). Similarly, the court in *Dusterhoft* rejected the plaintiffs' "assertion that, simply by contracting with [the plaintiffs'] healthcare insurers and providers, [the defendant] became a fiduciary with respect to

[the p]laintiffs,” and it also rejected the plaintiffs’ theory that the defendant’s privacy policy “suggest[ed] the existence of a fiduciary relationship.” 2024 U.S. Dist. LEXIS 170993, at *45–46.

Courts applying the laws of other states have similarly rejected the notion that an entity’s retention of PII, and accompanying assumption of a responsibility to protect it as expressed in a privacy policy, suffice to create a fiduciary relationship. *See, e.g., Cravens v. Garda CL Se., Inc.*, No. 24-CV-80400-RLR, 2024 U.S. Dist. LEXIS 227104, at *34–35 (S.D. Fla. Dec. 6, 2024) (rejecting the plaintiffs’ contention that “they had a fiduciary relationship with [the defendant] because ‘[the defendant] served as guardian of [the p]laintiffs’ . . . PII/PHI,’ and [the defendant] became a fiduciary by ‘undertaking to collect and maintain that PII/PHI’”); *Brooks v. Peoples Bank*, 732 F. Supp. 3d 765, 781 (S.D. Ohio 2024) (rejecting the plaintiffs’ argument that their “banking relationship” with the defendant, the bank’s “accepting and maintaining [the] [p]laintiffs’ PII,” and the bank’s “privacy policy statement on [its] website” sufficed to give rise to fiduciary duties); *Mgaresh v. Va. Union Univ.*, 3:24-cv-337-HEH, 2025 U.S. Dist. LEXIS 35926, at *2–3, *15–16 (E.D. Va. Feb. 27, 2025) (declining to find fiduciary relationship between former student applicants and university where former student applicants submitted PII to defendant university as part of application process and defendant university agreed to safeguard the data).

The Court will accordingly dismiss Plaintiff’s breach of fiduciary duty claim, and since amendment as to that claim would be futile, the dismissal will operate with prejudice. *See Circle Block Partners*, 44 F.4th at 1023 (citing *Runnion*, 786 F.3d at 519 and *Zimmerman*, 25 F.4th at 494).

4.2.8 WDTPA Claim

Defendant next moves the Court to dismiss Plaintiff's WDTPA claim. ECF No. 15 at 19–20. Plaintiff's WDTPA claim essentially asserts that Defendant falsely represented—“(affirmatively and/or by omission)” —to the public that it would keep sensitive PII confidential and that “as a direct and proximate result” of that false representation, Plaintiff suffered losses including having expended time monitoring her financial accounts for fraudulent activity. ECF No. 1 at 38–40.

“Claims arising under the [WDTPA] have three required elements: “(1) the defendant made a representation to the public with the intent to induce an obligation, (2) the representation was untrue, deceptive or misleading, and (3) the representation materially induced (caused) a pecuniary loss to the plaintiff.” *Weaver v. Champion Petfoods USA Inc.*, 3 F.4th 927, 934 (7th Cir. 2021) (quoting *Novell v. Migliaccio*, 749 N.W.2d 544, ¶ 44 (Wis. 2008)).¹² “Silence—an omission to speak—is insufficient to support a claim’ under the [WDTPA] and thus it applies ‘only [to] affirmative assertions, representations, or statements of fact that are false, deceptive, or misleading.’” *Id.* (quoting *Tietsworth v. Harley-Davidson, Inc.*, 677 N.W.2d 233, ¶ 40 (Wis. 2004)).

Defendant points out that Plaintiff's allegations of “omissions” fail to support a WDTPA claim. ECF No. 16 at 19–20. Plaintiff does not challenge that argument, stating only in her opposition that she “does not

¹²Plaintiff can only prevail on a WDTPA claim if she was a member of “the public” at the time of the misrepresentation. *Hinrichs*, 937 N.W.2d, ¶ 58 (quoting *K&S Tool & Die Corp. v. Perfection Mach. Sales, Inc.*, 732 N.W.2d 792, ¶ 19 (Wis. 2007)). Defendant does not contend that, based on her allegations, Plaintiff could not as a matter of law have been a member of “the public” for WDTPA purposes. Accordingly, the Court addresses this aspect of the analysis no further.

rely *solely* on omissions.” ECF No. 18 at 21 (emphasis added). Defendant is correct; Plaintiff’s allegations of representations “by omission,” ECF No. 1 at 38, do not support her WDTPA claim. *Weaver*, 3 F.4th at 934 (quoting *Tietzworth*, 677 N.W.2d, ¶ 40); *see also State v. McGuire*, 735 N.W.2d 555, ¶ 21 (noting that the WDTPA “provides no remedy for omissions of material facts”).

Defendant also argues that Plaintiff fails to allege “with particularity” that Defendant “made any specific misrepresentations to the public or Plaintiff regarding her data security.” ECF No. 15 at 19–20 (“As a claim sounding in fraud, Plaintiff’s claim must also be pleaded with particularity” (collecting cases)). Plaintiff does not challenge Defendant’s contention that Rule 9’s heightened pleading standard applies to this claim, *see* ECF No. 18 at 21, so any such argument has been forfeited. *See Platt*, 632 F. App’x at 295 (citation omitted). In any event, the contention finds some support in the caselaw. *See, e.g., Tangent Techs., LLC v. Recycled Plastics Indus., LLC*, No. 23-C-261, 2024 U.S. Dist. LEXIS 157277, at *28 (E.D. Wis. July 24, 2024). The Court will accordingly proceed under the assumption that the federal heightened pleading standard applies.¹³ “This

¹³Whether the heightened pleading standard does, in fact, apply is not entirely clear; the cases upon which Defendant relies in support of that contention all predate the Wisconsin Supreme Court’s decision in *Chris Hinrichs & Autovation Ltd. v. Dow Chemical Corp.*, in which the Wisconsin Supreme Court expressly clarified that “the heightened pleading standard set forth by Wis. Stat. § 802.03(3) for claims of fraud does not apply to claims made under Wis. Stat. § 100.18” 937 N.W.2d 37, ¶ 91 (Wis. 2020). That pronouncement is not dispositive, since “federal law establishes the pleading standard” in federal court, even for state law claims. *Caterpillar, Inc. v. Usinor Industeel*, 393 F. Supp. 2d 659, 670 (N.D. Ill. 2005) (citing *Guar. Residential Lending, Inc. v. Int’l Mort. Ctr., Inc.*, 305 F. Sup. 2d 846, 851 (N.D. Ill. 2004)). Nevertheless, at least one federal district court declined to apply the heightened pleading standard to a WDTPA claim post-*Hinrichs* since the Wisconsin Supreme Court expressly concluded that such a claim is “not a claim

ordinarily requires describing the ‘who, what, when, where, and how’ of the fraud.” *Perdue*, 455 F. Supp. 3d at 768 (quoting *Pirelli Armstrong Tire Corp. Retiree Med. Benefits Tr. v. Walgreen Co.*, 631 F.3d 436, 441–42 (7th Cir. 2011)).

The Court is satisfied that Plaintiff has sufficiently alleged that Defendant misrepresented via its privacy policy that it uses “reasonable and appropriate” security measures to protect PII, ECF No. 1 at 3–4, and that it uses “industry-standard . . . security measures and safeguards,” *id.* at 5, when in fact its cybersecurity system failed to follow FTC guidelines and meet industry standards, *id.* at 18–21. Plaintiff has sufficiently alleged that Defendant made those representations “to induce the public to disclose such information,” *id.* at 38, and that those representations were allegedly “untrue, deceptive or misleading.” *Weaver*, 3 F.4th at 934 (quoting *Novell*, 749 N.W.2d, ¶ 44); *see Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *57–58 (rejecting the defendant’s argument that the plaintiffs failed to allege that the defendant “made any misrepresentations regarding data security” where plaintiffs had alleged that the defendant “made a representation, via its website, that it ‘maintain[s] commercially reasonable security measures to protect [PII] [it] collect[s] and store[s] from loss, misuse, destruction, or unauthorized access’”); *see also Perdue*, 455 F. Supp. 3d at 769 (“Even assuming *arguendo* that the Rule 9(b) standard applies, [the] [p]laintiffs have alleged enough facts to establish who (the [d]efendant), what and how (security was inadequate to protect against a data breach and the information was withheld), when (the data breach occurred between

for fraud.” *T&M Farms v. CNH Indus. Am., LLC*, No. 19-C-0085, 2020 U.S. Dist. LEXIS 40727, at *34 n.6 (E.D. Wis. Mar. 5, 2020)).

November 2018 and August 2019), and where (respective [p]laintiffs' states).").

Lastly, Defendant argues that Plaintiff fails to allege that she heard or saw the alleged misrepresentation before turning over her PII and that any alleged misrepresentation "was a factor in her decision" to turn over her PII. ECF No. 15 at 19. This argument goes to the third element of a WDTA claim—that "the representation materially induced (caused) a pecuniary loss to the plaintiff." *Weaver*, 3 F.4th at 934 (quoting *Novell*, 749 N.W.2d, ¶ 44). This element ultimately requires the plaintiff to "prove . . . that [the defendant's] misrepresentation . . . caused [the plaintiff] to sustain a pecuniary loss." *K&S Tool & Die*, 732 N.W.2d, ¶ 34.

The Court agrees that Plaintiff has failed to plausibly allege that Defendant's alleged misrepresentations regarding its cybersecurity caused Plaintiff's pecuniary loss. That is so irrespective of whether the heightened pleading standard in fact applies to this claim. *See supra* note 13. There is no factual allegation in the complaint that suggests that Defendant's representations in its privacy policy played any role in Plaintiff's decision to disclose her PII. Plaintiff does not even allege that she saw or was otherwise made aware of Defendant's privacy policy before she agreed to disclose her PII. *See* ECF No. 20 at 17 (Defendant's reply) ("There is nothing in the Complaint that suggests Plaintiff knew the Privacy Policy existed before she filed this action."); *Dusterhoft*, 2024 U.S. Dist. LEXIS 170993, at *58–59 ("The . . . [c]omplaint does not plausibly allege . . . a causal connection between [the defendant's] alleged misrepresentations and any pecuniary loss by [the] [p]laintiffs. . . . [The] [p]laintiffs [do not] allege that they were aware of the alleged misrepresentations."). Plaintiff's WDTA claim accordingly must be dismissed. However, because the Court cannot

necessarily conclude that amendment as to this claim would be futile, the dismissal will operate without prejudice. *See Circle Block Partners*, 44 F.4th at 1023 (citing *Runnion*, 786 F.3d at 519 and *Zimmerman*, 25 F.4th at 494).

4.2.9 Wis. Stat. § 146.82 Claim

Lastly, Defendant moves the Court to dismiss Plaintiff's claim for breach of confidentiality of health records under Wis. Stat. § 146.82, *et seq.* ECF No. 15 at 20–21. Wis. Stat. § 146.82(1) provides, in relevant part, that “[p]atient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient,” subject to some exceptions that are not applicable here. Wis. Stat. § 146.84(1)(bm) creates a private right of action against anyone who negligently violates § 146.82(1).

Defendant argues that Plaintiff fails to plausibly allege that any “patient health care records”—as opposed to mere health information—were exposed in the data breach. ECF No. 15 at 20. The Court must agree. “[P]atient health care records” means, for purposes of § 146.82(1), “all records related to the health of a patient prepared by or under the supervision of a health care provider.” Wis. Stat. § 146.81(4). “The statutory definition does not encompass mere information that is not reduced to a record.” *Wall v. Pahl*, 886 N.W.2d 373, ¶ 28 (Wis. Ct. App. 2016) (citing *State v. Straehler*, 745 N.W.2d 431, ¶¶ 19–20 (Wis. Ct. App. 2008)).

To the extent that Plaintiff's complaint references any exposure of health care records, it does so vaguely and without any supporting detail or context such that the allegation is no more than a bare recitation of the element of the claim. *See* ECF No. 1 at 42 (“Defendant violated § 146.82 by, *inter alia*, failing to keep health care records confidential . . .”). Meanwhile, the complaint elsewhere references exposure of mere “medical

information” and “health insurance information,” *id.* at 7, the release of which does not give rise to a state law claim for breach of confidentiality of health records as a matter of law. *Wall*, 886 N.W.2d, ¶ 28. Plaintiff has not plausibly alleged that any patient health care records were exposed in the data breach, so her claim must be dismissed on that basis alone.¹⁴ But because this is an issue that could hypothetically be remediable by amendment, the dismissal of this claim will operate without prejudice. *See Circle Block Partners*, 44 F.4th at 1023 (citing *Runnion*, 786 F.3d at 519 and *Zimmerman*, 25 F.4th at 494).

5. CONCLUSION

For all these reasons, the Court grants in part and denies in part Defendant’s motion to dismiss, ECF No. 14. Plaintiff’s claims for negligence, negligence per se premised on an alleged FTCA violation, and unjust enrichment based on Defendant’s alleged receipt of payment may proceed. Plaintiff’s claims for declaratory and injunctive relief are dismissed without prejudice for lack of standing. The following claims are dismissed without prejudice for failure to state a claim: negligence per se premised on a HIPAA violation; breach of implied contract; claim under Wis. Stat. § 995.50(2)(am)(3) (publicity of private facts); WDTPA claim; and claim under Wis. Stat. § 146.82. Plaintiff’s claims under Wis. Stat. § 995.50(2)(am)(1), for breach of fiduciary duty, and of unjust enrichment premised on the conferral of PII are dismissed with prejudice.

¹⁴Because it dismisses the claim on this basis, the Court does not reach Defendant’s additional argument that Plaintiff fails to allege “an actual ‘release’” under the statute. ECF No. 15 at 21. Should Plaintiff file an amended complaint in which she repleads her § 146.82 claim and remedies the pleading deficiency addressed herein, Defendant may renew its motion to dismiss this claim on the basis of that argument.

Should Plaintiff wish to amend her complaint to attempt to remedy the deficiencies discussed herein as to the claims subject to dismissal without prejudice, she may do so on or before **May 22, 2025**. If Plaintiff chooses not to amend her complaint, or fails to do so on a timely basis, this action will proceed only as to her claims of negligence, negligence per se premised on an alleged FTCA violation, and unjust enrichment based on Defendant's alleged receipt of payment.

Accordingly,

IT IS ORDERED that Defendant MRA – The Management Association, Inc.'s motion to dismiss, ECF No. 14, be and the same is hereby **GRANTED in part and DENIED in part** as stated herein;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's claim for declaratory relief, ECF No. 1 at 42–43 (ninth cause of action), be and the same is hereby **DISMISSED without prejudice** for lack of standing;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's request for injunctive relief, ECF No. 1 at 43, be and the same is hereby **DISMISSED without prejudice** for lack of standing;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's claim of negligence per se, ECF No. 1 at 29–30 (second cause of action), be and the same is hereby **DISMISSED without prejudice** to the extent that it is premised on an alleged violation of HIPAA;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's breach of implied contract claim, ECF No. 1 at 30–33 (third cause of action) be and the same is hereby **DISMISSED without prejudice**;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's invasion of privacy claim under Wis. Stat. § 955.50(2), ECF No. 1 at 33–35 (fourth cause of action), be and the same is hereby **DISMISSED**; to the extent that

that claim was premised on subsection (am)(1), it is **DISMISSED with prejudice**; to the extent that the claim was premised on subsection (am)(3), it is **DISMISSED without prejudice**;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's unjust enrichment claim, ECF No. 1 at 35–37 (fifth cause of action), be and the same is hereby **DISMISSED with prejudice** solely to the extent that it is premised in the alleged benefit of Defendant using Plaintiff's PII/PHI to facilitate its business, ECF No. 1 at 36; to the extent that her unjust enrichment claim is premised on Defendant's alleged receipt of payment, ECF No. 1 at 36, the claim may proceed;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's breach of fiduciary duty claim, ECF No. 1 at 37–38 (sixth cause of action), be and the same is hereby **DISMISSED with prejudice**;

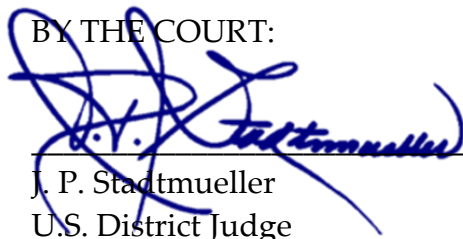
IT IS FURTHER ORDERED that Plaintiff Susan Giasson's Wisconsin Deceptive Trade Practices claim, ECF No. 1 at 38–40 (seventh cause of action), be and the same is hereby **DISMISSED without prejudice**;

IT IS FURTHER ORDERED that Plaintiff Susan Giasson's claim for breach of confidentiality of health records under Wis. Stat. § 146.82, ECF No. 1 at 40–42 (eighth cause of action), be and the same is hereby **DISMISSED without prejudice**; and

IT IS FURTHER ORDERED that Plaintiff Susan Giasson shall file an amended complaint, if at all, on or before **May 22, 2025**.

Dated at Milwaukee, Wisconsin, this 7th day of April, 2025.

BY THE COURT:



J. P. Stadtmueller
U.S. District Judge